AFTER FINAL EXPEDITED PROCEDURE

REMARKS

Claims 1 to 20 were pending in the application at the time of final examination. The final restriction requirement was maintained. Claims 1 to 4, 6 to 9, 11 to 14, and 16 to 19 remain rejected as obvious.

Restriction Requirement

The finality of the restriction requirement was maintained. First, Applicants note that MPEP § 806.05 includes more requirements than those for a combination and subcombination. Therefore, citation to specific subsections of this section was not demonstrating any support for the incorrect characterization of the claims in the restriction requirement. In particular, Applicants pointed out that "806.05(j) Related Products; Related Processes," which did not support the characterization in the rejection, but did support the Applicant's Remarks that the MPEP does in fact draw a distinction between subcombinations and processes of making and using a product. Second, the rationale for maintaining the finality stated in part:

> The invention of group I (claims 1-4, 6-9, 11-14, and 16-20) contain limitations not found in group II (claims 5, 10, 15, and 20) and vice versa, thus the inventions are two way distinct.

Applicants respectfully submit that this showing fails to demonstrate two-way distinctness. Different claim limitations are not sufficient. Using this criterion, two claims that varied in scope would be distinct because each claim included limitations not found in the other claim. However, if such claims were obvious variants despite the different limitations, the claims would not be distinct. If two processes did not include different claim limitations, there would be no need for the demonstration by the Office of two-way distinctness,

Page 2 of 9

Appl. No. 10/672,184
Amdt. dated January 24, 2008
Reply to Final Office Action of November 26, 2007

AFTER FINAL EXPEDITED PROCEDURE

because the two sets of claims would clearly be directed at the
same invention. Thus not every set of two processes that
includes different claim limitations is distinct. Therefore,
the rationale for maintaining the finality does not form a
proper basis for the requirement. Thus, there still is no
basis on the record for the restriction that meets the
requirements of the MPEP and restriction should be withdrawn.
Applicant respectfully requests reconsideration and withdrawal
of the restriction requirement.

§ 103 Rejections

Claims 1-2, 4, 6-7, 9, 11-12, 14, 16-17, and 19 stand
rejected under 35 U.S.C. 103(a) as being unpatentable over
Kessler et al U. S. Patent No. 7,170,999, hereinafter referred
to as Kessler, in view of U.S. Patent No. 6,789,177,
hereinafter referred to as Okada, further in view of PCT
Publication No. WO 02/079955, herein after referred to as Orr,
and in further view U.S. Patent Application Publication No.
2002/0120854), herein after referred to as Levine.

Applicant respectfully traverses the obviousness rejection
of Claims 1, 6, 11 and 16. Applicant respectfully submits that
still neither the references nor the claims have been
considered as a whole as required by the MPEP in an obviousness
rejection and that the basis for the combination of references
is not well founded.

The rejection confuses two parts of Kessler and appears to
arbitrarily extract teachings from different parts and then
recombine them. This is error, because such a recombination
changes the principles of operation of Kessler. Specifically,
the MPEP provides:

> If the proposed modification or combination of the prior art would
> change the principle of operation of the prior art invention being
> modified, then the teachings of the references are not sufficient to
> render the claims *prima facie* obvious.

Page 3 of 9

Appl. No. 10/672,184
Amdt. dated January 24, 2008
Reply to Final Office Action of November 26, 2007

AFTER FINAL EXPEDITED PROCEDURE

MPEP §2143.01 VI., 8th Ed., Rev. 6, pg. 2100-141, (Sept. 2007).

Specifically, the rejection relies upon the proprietary client software and teachings about how a key TK is processed to support file transfer in a peer to peer network. These are two different and distinct things as taught by Kessler.

With respect to the proprietary client software, Kessler taught:

> A system for and method of securely transferring files within a distributed environment includes client computers loaded with proprietary software capable of performing secure file transfers.

Kessler, Col. 3, lines 22 to 24.

> As registered client computers, each computer within the distributed environment receives proprietary software to facilitate the file transfer process.

Kessler, Col. 3, lines 43 to 45.

> As part of the registration process, the client computer receives proprietary client software for facilitating the file sharing process. The client software includes a unique secret key, SK, and a unique public key, PK, for each registered client computer. . . . The secret key and the public key are embedded within the client software such that neither are accessible by the user of the client computer. Such secure measures prevents unauthorized use of the secret key to decrypt the transferred data.

Kessler, Col. 4, lines 44 to 62.

> As previously discussed, each registered client computer receives proprietary client software. The proprietary client software includes the public key, the secret key and the necessary encryption and decryption algorithms. The public key and the secret key are unique to each client computer. To provide additional security, the proprietary client software also includes obfuscation and de-obfuscation algorithms. The obfuscation algorithm employs mathematical transforms that scramble data. Before a file is encrypted using the transfer key, TK, the file is obfuscated. The obfuscation algorithm is the same algorithm on each client computer. The de-obfuscation algorithm is used to de-obfuscate an obfuscated

Appl. No. 10/672,184
Amdt. dated January 24, 2008
Reply to Final Office Action of November 26, 2007

AFTER FINAL EXPEDITED PROCEDURE

file. The obfuscation algorithm, the de-obfuscation algorithm, the secret key, and the public key are themselves obfuscated and/or encrypted within the proprietary client software used by the client computer. In this manner, users are unable to perform de-obfuscating and decrypting that might lead to unauthorized file sharing.

Kessler, Col. 8, lines 50 to 67.

The obfuscation algorithms O1 and O2, and the associated de-obfuscation algorithms DO1 and DO2, are the same on each registered client computer. The algorithms O1, O2, DO1, and DO2 are bound within the proprietary client software loaded onto the registered client computers. The algorithms O1, O2, DO1, and DO2 are themselves obfuscated within the computer code of the proprietary client software.

Kessler, Col. 8, lines 50 to 67.

While Kessler stated that the "obfuscation algorithm, the de-obfuscation algorithm, the secret key, and the public key are themselves obfuscated and/or encrypted within the proprietary client software," Kessler fails to teach how this was done. The rejection has cited no teaching in Kessler of how the various elements are obfuscated and/or encrypted within the proprietary client software before that software is transferred to a client. The fact that Kessler makes a general statement, as quoted above, provides no suggestion or teaching of how to implement the proprietary client software or what process was used. Clearly, Kessler is trying to protect the obfuscation of the proprietary client software so that the patent cannot be used as a vehicle to overcome the protection that is sought by use of the obfuscation of the proprietary client software.

Moreover, Kessler clearly describes that the key TK is not included in the proprietary client software. Rather, Kessler taught that the key TK is generated and used in transfer of a file in the peer to peer network. For example, Kessler states multiple times "User 1 generates a track key, TK, for this particular file transfer." Thus, the key TK is separate and

CUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0800
Fax (831) 655-0888

Page 5 of 9

Appl. No. 10/672,184
Amdt. dated January 24, 2008
Reply to Final Office Action of November 26, 2007

                                    AFTER FINAL EXPEDITED PROCEDURE

distinct from the proprietary client software and not included
in that software. Thus, combination of the proprietary client
software and the key TK changes the principles of operation of
Kessler because there has been no citation of an encrypted key
TK being scrambled with the proprietary client software. Thus,
in view of the above quote from the MPEP, the recombination of
Kessler, as was done in the rejection, is improper.

In addition, the rationale for continuing the rejection
clearly did not consider the plain meaning of these Claims.
For example, Claim 1 recites in part:

> scrambling . . . said encrypted second cryptographic key into
> said instruction stream using a code obfuscation method indicated by
> an obfuscation descriptor

Thus, the Claims recite that the encrypted second
cryptographic key is scrambled. Further, it is not scrambling
in general, but rather the scrambling is done using a code
obfuscation method. Further, the code obfuscation method is
not just any such method, but rather the code obfuscation
method is the method indicated by an obfuscation descriptor.
Finally, the scrambling is done with respect to a specific
entity, the instruction stream. The result of the scrambling
of the encrypted second cryptographic key using the specific
code obfuscation method not only obfuscates the key but also
generates "an obfuscated key decryption program".

This follows directly from the plain meaning of the claim.
Nevertheless, the rationale for continuing the rejection
stated:

> It is noted that the next to last limitation in claim 1, for example,
> recites that an encrypted second key is scrambled into said
> instruction stream using a code obfuscation method to create an
> obfuscated key decryption program. However, the limitation appears to
> require that the instruction stream be obfuscated, not the encrypted
> second key. Just because the encrypted second key was used as an
> input into an obfuscation method does not mean that it was the key
> that was obfuscated.

                                    Page 6 of 9

Appl. No. 10/672,184
Amdt. dated January 24, 2008
Reply to Final Office Action of November 26, 2007

AFTER FINAL EXPEDITED PROCEDURE

The claim language specifically recites that the encrypted key is scrambled. The interpretation in the rejection has nothing to do with the explicit claim language. Moreover, it ignores the level of skill in the art as demonstrated by Kessler. As quoted above, Kessler taught "The obfuscation algorithm employs mathematical transforms that scramble data." Thus, Kessler taught that scrambling data was a method of obfuscation. Therefore, Applicant's interpretation of the express claim language is totally consistent with knowledge of one of skill in the art.

The rejection still has not clearly identified an instruction stream that is a key decryption program configured to perform said decryption algorithm for said first cryptographic key and that has an encrypted key scrambled into the instruction stream to obtain an obfuscated instruction stream. The key TK is taught only as being encrypted and not scrambled. The key TK is not included in the proprietary client software. Kessler specifically considered the need for obfuscation and taught that obfuscation of the encrypted key TK was unnecessary and failed to suggest or disclose the specific scrambling recited in this claim.

Further, the rejection arbitrarily mixes and matches key from other processes into Kessler. This is error. Again, the MPEP states:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.

MPEP §2143.01 VI., 8th Ed., Rev. 6, pg. 2100-141, (Sept. 2007).

Kessler taught that the public key PK, secret key SK combination was needed to make the file transfer work. While other key combinations might improve performance locally, they break Kessler because the public key PK and secret key SK

Appl. No. 10/672,184
Amdt. dated January 24, 2008
Reply to Final Office Action of November 26, 2007

AFTER FINAL EXPEDITED PROCEDURE

combination is gone. Kessler bases the entire process on this combination and so not only are the principles of operations of Kessler changed, but also, there has been no showing of why Kessler would be expected to work for its intended purpose, secure peer to peer file transfer, after such a change.

> If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

MPEP §2143.01 V., 8th Ed., Rev. 6, pg. 2100-140, (Sept. 2007). It is respectfully submitted that when the keys used in the encryption and decryption of Kessler are changed, Kessler is rendered unsatisfactory for its intended purposes because the public key and its specific relationship to the secret key SK is described as being required in the process. Therefore, the MPEP directs that in addition to the basic deficiencies of Kessler, there is no motivation for the combinations.

The rejection continues to confuse this proprietary client software with the process for transferring files between clients as taught by Kessler. Therefore, when considered as a whole, Kessler has been mischaracterized and misinterpreted in the rejection. Properly interpreted, Kessler teaches away from the Applicant's claims as well as the motivation for the modifications to Kessler.

Any one of these distinctions is sufficient to overcome the obviousness rejection. Therefore, Applicant respectfully requests reconsideration and withdrawal of the obviousness rejection of each of Claims 1, 6, 11 and 16.

With respect to each of the claims dependent from Claims 1, 6, 11 and 16, the additional material relied upon from the secondary references, or the new reference with respect to Claims 3, 8, 13 and 18, does not correct the deficiencies of the combination of references with respect to the independent claims from which these claims depend. Therefore, each of

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-9800
Fax (831) 655-0888

Page 8 of 9

Appl. No. 10/672,184
Amdt. dated January 24, 2008
Reply to Final Office Action of November 26, 2007

AFTER FINAL EXPEDITED PROCEDURE

Claims 2 to 4, 7 to 9, 11 to 14 and 17 to 19 distinguish over the combination of references for at least the same reasons as the independent claims. Applicant respectfully requests reconsideration and withdrawal of the obviousness rejection of each of Claims 2 to 4, 7 to 9, 11 to 14 and 17 to 19.

Claims 1 to 20 remain in the application. For the foregoing reasons, Applicant(s) respectfully request allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

Respectfully submitted,

CERTIFICATE OF TRANSMISSION
I hereby certify that this correspondence is being facsimile transmitted to the U.S. Patent and Trademark Office, Fax No. (571) 273-8300, on January 24, 2008.

Mona Marshall   January 24, 2008
Mona Marshall   Date of Signature

Forrest Gunnison
Attorney for Applicant(s)
Reg. No. 32,899

Page 9 of 9